



Release Notes for VPN Client, Release 3.6 Through Release 3.6.5

CCO Date: July 17, 2003

Part Number 78-15450-02



Note

You can find the most current documentation for the VPN Client at <http://www.cisco.com> or <http://cco.cisco.com>. These electronic documents may contain updates and changes made after the hard copy documents were printed.

These release notes support VPN Client software Release 3.6 and all of its incremental “point” releases through Release 3.6.5. Please note that product release numbers are not necessarily consecutive. These release notes describe new features, limitations and restrictions, interoperability notes, caveats, and related documentation. Please read the release notes carefully prior to installation. A new section, “Usage Notes,” describes interoperability considerations and other issues you should be aware of when installing and using the VPN Client.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003. Cisco Systems, Inc. All rights reserved.

Contents

- [Introduction, page 3](#)
- [System Requirements, page 3](#)
- [Installation Notes, page 5](#)
- [New Features in Release 3.6.1 Through 3.6.3.B, page 9](#)
- [Usage Notes, page 13](#)
- [Open Caveats, page 28](#)
- [Caveats Resolved in Release 3.6.5, page 41](#)
- [Caveats Resolved in Release 3.6.4.A, page 41](#)
- [Caveats Resolved in Release 3.6.4, page 42](#)
- [Caveats Resolved in Release 3.6.3.C, page 44](#)
- [Caveats Resolved in Release 3.6.3.B, page 45](#)
- [Caveats Resolved in Release 3.6.3, page 50](#)
- [Caveats Resolved in Release 3.6.2.B, page 51](#)
- [Caveats Resolved in Release 3.6.2.A, page 52](#)
- [Caveats Resolved in Release 3.6.2, page 53](#)
- [Caveats Resolved in Release 3.6.1, page 54](#)
- [Caveats Resolved in Release 3.6, page 55](#)
- [Documentation Updates, page 63](#)
- [Related Documentation, page 64](#)
- [Obtaining Documentation, page 64](#)
- [Obtaining Technical Assistance, page 66](#)

Introduction

The VPN Client is a set of software applications that runs on a Microsoft® Windows®-based PC, a Sun ultraSPARC workstation, or a Macintosh personal computer that meets the system requirements stated in the next section. In this document, the term “PC” applies generically to all these computers, unless specified otherwise.

The VPN Client on a remote PC, communicating with a Cisco VPN device at an enterprise or service provider, creates a secure connection over the Internet that lets you access a private network as if you were an on-site user. This secure connection is a Virtual Private Network (VPN).

System Requirements

Refer to Chapter 2, “Installing the VPN Client,” in the *VPN Client User Guide for Windows, Release 3.6* or *Cisco VPN Client User Guide for Linux, Solaris, and Mac OS X*, as appropriate for your platform, for a complete list of system requirements and installation instructions.

- To install the VPN Client on *any* system, you need
 - CD-ROM drive (if you are installing from CD-ROM)
 - Administrator privileges
- The following table indicates the system requirements to install the VPN Client on each of the supported platforms.

Computer	Operating System	Requirements
Computer with a Pentium®-class processor or greater	<ul style="list-style-type: none"> Microsoft® Windows® 95 (OSR2), Windows 98, or Windows 98 (second edition) Windows ME Windows NT® 4.0 (with Service Pack 6, or higher) Windows 2000 Windows XP 	<ul style="list-style-type: none"> Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.) 10 MB hard disk space. RAM: <ul style="list-style-type: none"> 16 MB for Windows 95/98 32 MB for Windows NT and Windows ME 64 MB for Windows 2000 128 MB for Windows XP
Computer with and Intel x86 processor	RedHat Version 6.2 or later Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later Note The VPN Client does not support Linux kernel Version 2.5.	<ul style="list-style-type: none"> 32 MB Ram 10 MB hard disk space
Sun UltraSPARC computer	32-bit or 64-bit Solaris kernel OS Version 2.6 or later	<ul style="list-style-type: none"> 32 MB Ram 10 MB hard disk space
Macintosh computer	OS X, Version 10.1.0 or later	5 MB hard disk space

The Cisco VPN Client supports the following Cisco VPN devices:

- Cisco VPN 3000 Concentrator Series, Version 3.0 and later.
- Cisco PIX Firewall, Version 6.1 (1) and later.
- Cisco IOS Routers, Version 12.2(8)T and later

Installation Notes

Because of platform differences, the installation instructions for Windows and non-Windows platforms also differ.

- Refer to the *VPN Client User Guide for Windows, Release 3.6*, Chapter 2, for complete installation instructions for Windows users.
- Refer to the *Cisco VPN Client user Guide for Linux, Solaris, and Mac OS X*, Chapter 2, for complete installation information for those platforms.

The following notes are important for users who are upgrading to Windows XP and users who want to downgrade to an earlier version of the VPN Client software.

Installation Changes - Windows Platforms

Release 3.6.x includes the following new installation changes for Windows users:

- The VPN Client no longer replaces the system GINA during the installation process. If you enable the “Start Before Logon” feature (available on Windows NT, Windows 2000, and Windows XP Professional Edition, but not on Windows XP Home Edition), the VPN Client automatically replaces and links to the original GINA.
- Windows Installation Package (MSI) is now available for Windows NT (SP6), Windows 2000, and Windows XP.

Installing the VPN Client Software Using InstallShield

Installing the VPN Client software on Windows NT, Windows 2000, or Windows XP with InstallShield requires Administrator privileges. If you do not have Administrator privileges, you must have someone who has Administrator privileges install the product for you.

Installing the VPN Client Software Using the MSI Installer

If you are using the MSI installer, you must have Windows NT-based products such as Windows NT 4.0 (with SP6), Windows 2000, or Windows XP. Installing with MSI also requires Administrator privileges.

VPN Client Installation Using Windows Installer (MSI) Requires Windows NT SP6

When you attempt to install the VPN Client using MSI install (vpnclient_en.exe) on NT SP3, SP4, or SP5, the error messages do not indicate that the VPN Client cannot be installed on those operating systems because they are unsupported. Once the errors occur, no other messages are displayed and the installation is aborted.

When you attempt to run vpnclient_en.exe on Windows NT SP3, SP4, or SP5 you see the following messages:

“Cannot find the file instmsiw.exe (or one of its components). Make sure the path and filename are correct and that all the required libraries are available.”

-then-

“Cannot find the file MSIEXEC (or one of its components). Make sure the path and filename are correct and that all the required libraries are available.”

The Windows Installer (MSI) can be installed only on NT SP6, so the error messages you see using earlier service packs are due to an MSI incompatibility (CSCdy05049).

Close All VPN Client Applications Before Uninstalling the VPN Client.

If one of the VPN Client applications is running while the VPN Client is being uninstalled, a message box appears giving the following three choices: Cancel, Retry, Ignore.

If you select Ignore, the application continues running, but the VPN Client and all applications are uninstalled. When the computer reboots, the application is no longer on the hard drive (CSCdx42035).

Installation Notes - Solaris Platforms

The following sections describe actions you must take when installing the VPN Client on a Solaris platform.

Uninstall an Older VPN Client If Present on a Solaris Platform

If you have a previous version of the VPN Client running under Solaris, you *must* uninstall the older VPN Client before installing a new VPN Client. You are not required to uninstall an old VPN Client, if one is present, *before* installing a new VPN Client for Linux or Mac OS X.

Refer to the *Cisco VPN Client User Guide for Linux, Solaris, and Mac OS X*, Chapter 2, for complete uninstallation information.

Disable the ipfilter Firewall Kernel Module Before Installing the VPN Client on a Solaris Platform

If you have an IP firewall installed on your workstation, the reboot after installation of the VPN Client takes an inordinate amount of time. This is caused by a conflict between the vpnclient kernel module cipsec and the ipfilter firewall module. To work around this issue, disable the ipfilter firewall kernel module before you install the VPN Client (CSCdw27781).

Using the VPN Client

- To use the VPN Client, you need
 - Direct network connection (cable or DSL modem and network adapter/interface card), or
 - Internal or external modem, and
 - For Windows 95, Microsoft Dial-Up Networking (DUN) version 1.2 or greater. (DUN 1.3 for Windows 95 is a recommended performance and security upgrade, and it is available as a free download from the Microsoft Web site, www.microsoft.com. Windows 98 includes the DUN 1.3 function.)

**Note**

The VPN Client may have data transfer problems if installed on a Windows 95a system. We recommend that you do not use the VPN Client on Windows 95a. If you must use Windows 95 instead of a more recent version, make sure that you are using Windows 95 OSR+.

To check the version of Windows you have, open the Control Panel | System | General tab and look for the System version. Windows 95a is: 4.00.950a (CSCdt07587)

- To connect using a digital certificate for authentication, you need a digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC:
 - Baltimore Technologies (www.baltimoretechnologies.com)
 - Entrust Technologies (www.entrust.com)
 - Netscape (www.netscape.com)
 - Verisign, Inc. (www.verisign.com)
 - Microsoft Certificate Services — Windows 2000
 - A digital certificate stored on a smart card. The VPN Client supports smart cards via the MS CAPI Interface.

Windows XP Requires VPN Client Release 3.1 or Higher

If you are running Windows XP on your PC, you *must* upgrade your VPN Client to Release 3.1 or higher. VPN Client Release 3.0 does not support Windows XP.

If you are running the VPN Client on a PC and you want to upgrade your operating system to Windows XP, you must *first* uninstall the VPN Client, then install Windows XP, then install the VPN Client.

New Features in Release 3.6.1 Through 3.6.3.B

These release notes update the VPN Client to resolve several outstanding caveats. Refer to the appropriate “Caveats Resolved in Release 3.6.x” of these release notes for details on each release.

New Features in Release 3.6

Release 3.6 of the VPN Client software includes the following new features.

Dynamic DNS

The VPN Client sends its hostname to the VPN Concentrator during connection establishment. The VPN Concentrator can send the hostname in a DHCP request that can cause a DNS server to update its database to include the new hostname and Client address.

Split DNS

Release 3.6 has the ability to direct packets in clear text over the Internet to domains served through an external DNS (serving your ISP) or through an IPSec tunnel to domains served by the corporate DNS. The VPN Server supplies a list of domains to the VPN Client for tunneling packets to destinations in the private network.

For example, a query for a packet destined for *corporate.com* would go through the tunnel to the DNS that serves the private network, while a query to for a packet destined for *myfavoritesearch.com* would be handled by the ISP’s DNS. This feature is configured on the VPN Server (VPN Concentrator) and enabled on the VPN Client by default.

AES (Existing DH Groups)

Advanced Encryption Standard is an encryption algorithm, recently approved by NIST, for securing sensitive but unclassified material by U.S. Government agencies. AES applies mostly to the VPN Concentrator, where new default IKE proposals and IPSec SAs have been added. The VPN Client can use AES in establishing remote access connections with the VPN Concentrator. On the VPN Client, AES shows up as an Encryption in use on connection status screens. We support AES-128 and AES-256 key sizes.



Note

The VPN Client still supports DES/MD5; however, support for DES/SHA is no longer available. Because of the latter, Release 3.6 VPN Clients cannot connect to any central-site device group that is configured for (or proposing) DES/SHA. The VPN Client must either connect to a different group or the administrator for the central-site device must change the configuration from DES/SHA to DES/MD5 or another supported configuration. The *VPN Client Administrator Guide* lists all the supported encryption configurations.

Auto Initiation of VPN in a Wireless Environment

The Cisco VPN Client can be configured to automatically initiate a VPN based on the network that the user's machine is connected to (that is, based on a user's assigned address). This feature is called Auto Initiation for on-site Wireless LANs (WLANs).

The auto initiation feature was designed to make the user experience more like a traditional wired network in those environments in which VPNs are being used to secure WLANs. These environments are also known as on-site WLANs.

NAT Traversal (NAT-T), Including Auto-detect

NAT-T lets the VPN Client and the VPN Concentrator automatically detect when to use IPSec over UDP to work properly in Port Address Translation environments. NAT-T is an IPSec Working Group draft: draft-ietf-ipsec-nat-t-ike-02. See the *VPN Client Administrator Guide*, Chapter 1, for instructions on how to configure this feature on the VPN Concentrator.

Update of Centrally-Controlled Backup Server List

VPN Client can learn the backup VPN Concentrator list during connection establishment. This feature is configured on the VPN 3000 Concentrator and pushed to the VPN Client. The addresses show in the VPN Dialer application in the Enable Backup Servers box under Options->Properties->Connections.

Peer Certificate Distinguished Name Field Verification

This feature prevents a client from connecting to a valid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the Distinguished Name of the peer certificate fails, the client connection also fails. There is no user-visible change for this feature, but it requires a change to the connection profile.

New Global Profile Configuration Parameters (vpnclient.ini)

Release 3.6 adds the following new global profile configuration parameters under [Main]:

AutoInitiationEnable	Enables or disables auto initiation. To enable auto initiation, enter 1. To disable it, enter 0.
AutoInitiationRetryInterval	Specifies the number of minutes to wait before retrying an auto initiation connection. The range is 1 to 10 minutes. The default retry interval is one minute.
AutoInitiationList	Provides a series of section names, each of which contains a network address, a subnet mask, and a connection entry name. The network and subnet mask identify a subnet. The connection entry specifies a connection entry profile (.pcf file). You can include a maximum of 64 section (network) entries.

See the *VPN Client Administrator Guide, Release 3.6* for examples of using these parameters.

Creating Profiles for Client Users — New Parameters:

Release 3.6 adds the new keyword `VerifyCertDN` under `[Main]` for defining client profiles in the `*.pcf` file. This keyword prevents a user from connecting to a valid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the Distinguished Name of the peer certificate fails, the client connection also fails.



Note

In the `*.pcf` file, do not set the `DHgroup` parameter to 1.

New Parameters for Customizing the VPN Client Software

Release 3.6 adds new parameters to the `oem.ini` file for customizing the VPN Client software. For information about these parameters, see the *VPN Client Administrator Guide*, Chapter 5.

Stateful Firewall (Always On) Allows Inbound Tunneled Access

A Stateful Firewall (Always On) now allows inbound access from the internal (tunneled) network to ensure that system management applications work properly, while still providing additional protection by blocking all non-tunneled inbound traffic.

MSI - Microsoft Installer (Windows Installer) Support

MSI - Microsoft Installer (Windows Installer) package is now available for Windows NT, 2000, and XP. This package assists in packaging and customizable installation on these systems. This package is available in addition to the InstallShield installation package, which supports Windows desktop platforms.

Solaris 64-bit Support

The VPN Client now operates on Solaris UltraSPARC 64-bit systems.

Usage Notes

This section lists issues to consider before installing Releases 3.6 through 3.6.3 of the VPN Client software.

In addition, you should be aware of the open caveats regarding this release. Refer to “Open Caveats” on page 28 of these Release Notes for the list of known problems.

Potential Application Compatibility Issues

You might encounter the following compatibility issues when using the VPN Client with specific applications. Whenever possible, this list includes a description of the circumstances under which an issue might occur and workarounds for potential problems.

Windows Interoperability Issues

The following known issues might occur with the indicated Microsoft Windows operating systems and applications software.

WINS Support

On Windows 95 and Windows 98, dynamic WINS support works with DHCP-enabled adapters (for example, PPP or NIC adapters that get their IP information dynamically). For static configurations, users must manually configure the adapters with WINS information.

Windows NT

Users running Windows NT 4.0 with Service Pack 4 require a hot fix from Microsoft for proper operation. This fix is available on the Microsoft GetHostByName API Returns Unbindable Address page:
<http://support.microsoft.com/support/kb/articles/Q217/0/01.ASP>.

Importing a Microsoft Certificate Using Windows NT SP3

The following problem has occurred on some Windows NT SP3 systems (CSCdt11315).

When using the Client with digital certificates stored in the Microsoft certificate store, the Client may fail to connect. This is accompanied by the following Client event in the Log Viewer:

```
4101 13:41:48.557 01/05/01 Sev=Warning/2 CERT/0xA3600002
Could not load certificate (null) from the store.
```

Workaround: Two workarounds exist. Choose one of the following:

- Import the certificate from the Microsoft certificate store into the Cisco certificate store using the Cisco Certificate Manager. Refer to “Importing a Certificate” in the *VPN Client User Guide for Windows, Release 3.6*, Chapter 6.
- Alternatively, upgrade to a Windows Service Pack later than SP3.

VPN Client Cannot Launch Microsoft Connection Manager

The VPN Client does not see a dialup connection made with Microsoft Connection Manager because of incompatibilities between the requirements of the two applications (CSCdx85663).

Cannot Simultaneously Run the Cisco VPN Client and Windows 2000 Client

When switching between the Cisco VPN Client and the Windows 2000 L2TP/IPSec client, follow these steps (CSCdt84026):

-
- | | |
|---------------|--|
| Step 1 | Stop the Cisco VPN service and driver. At the command prompt, enter:
<pre>net stop cvpnd net stop cvpndrv</pre> |
| Step 2 | Enable the MS IPSec service (IPSec Policy Agent) by entering:
<pre>net start policyagent</pre> |
-

Windows 98 Might Hang on Shutdown

On some Windows 98 PCs with the VPN Client installed, if you restart the PC, it may stop responding (that is, “hang”) on the screen that says “Windows is shutting down”.

Wait a minute. If the PC is still not responding, press the reset button. When the PC reboots, it should not run through ScanDisk, indicating the shutdown was successful in closing all open files. This problem may occur on some PCs and not on others, and we are looking for a solution. Windows 98 shutdown has numerous issues, as can be seen the following Microsoft Knowledge Base Article:

“Q238096 - How to Troubleshoot Windows 98 Second Edition Shutdown Problems” (CSCdt00729).

Windows 2000 (only) Requires Adding Client for MS Networks for Dialup Connections

For the Cisco VPN Client running on a Windows 2000 system, you cannot access Microsoft resources unless you add the Client for Microsoft Networks for the Dial-up adapter.

Aladdin Runtime Environment (RTE) Issue with Windows NT and Windows 2000

Using versions of the Aladdin Runtime Environment (RTE) on Windows NT and Windows 2000 can cause the following behavior. The login prompt that is posted by the Aladdin etoken when connecting the VPN Client can get hidden in the background. If this happens, the VPN connection can timeout and fail with the following event:

“System Error: Connection Manager failed to respond.”

A side effect of this is that the VPN Client’s service and dialer might become out of synch, and the PC might need to be restarted (CSCdv47999). To avoid this issue, use the Aladdin Runtime Environment (RTE) version 2.65.

Microsoft MSN Installation

Microsoft’s MSN installation fails if you have already installed the VPN Client. Uninstall the VPN Client before you install MSN. After MSN has completed installation, you can install the VPN Client.

VPN Client Might Not Be Removed from Windows Servers If Not Disconnected Before Shutdown

The VPN Client on Windows NT or Windows 2000 WINS servers may not be removed if the PC is shut down without disconnecting the VPN Client and the “Disconnect VPN connection when logging off” feature is disabled.

If the VPN Concentrator is configured to send WINS server addresses down to the VPN Client and the PC is shut down or restarted without first disconnecting the VPN Client, the WINS servers are not removed from the network properties. This might cause local PC registration and name resolution problems while not connected with VPN.

To work around this problem, do *one* of the following:

- Be sure to disconnect the VPN Client before shutting down. If you are having problems, check your network properties and remove the WINS entries if they are not the correct ones for your network.
- Alternatively, enable “Disconnect VPN connection when logging off”. Go to Options > Windows Logon Properties, check Disconnect VPN connection when logging off (CSCdv65165).

VPN Client May Falsely Trigger Auto Initiation Connection Event though the NIC Card Has Been Removed

The 3.6 VPN Client with Auto Initiation enabled on a Windows NT system may exhibit the following behavior. After removing a NIC card, the VPN Client may continue to trigger an Auto Initiation connection event though the NIC card has been removed. To stop its connection attempts, you can place the VPN Client in Suspended mode after a failed or canceled VPN connection. You can also disable this feature from the GUI by using Options > Automatic VPN Initiation, and unchecking “Enable”. If you add a new NIC, the problem goes away. (CSCdx46812).

Allowing the VPN Client to Work Through ESP-Aware NAT/Firewalls

When using the VPN Client behind an ESP-aware NAT/Firewall, the port on the NAT/Firewall device may be closed due to the VPN Client’s keepalive implementation, called DPD (Dead Peer Detection). When a Client is idle, it does not send a keepalive until it sends data and gets no response.

To allow the VPN Client to work through ESP-aware NAT/Firewalls, add the following parameter and setting to the [Main] section of any *.pcf (profile configuration file) for the affected connection profile.

ForceKeepAlives=1

This parameter enables IKE and ESP keepalives for the connection at approximately 20 second intervals.

For more information, see “Connection Profile Configuration Parameters” in the *VPN Client Administrator Guide, Release 3.6*.

DNS

For DNS resolution, if the DOMAIN NAME is not configured on the network interface, you need to enter the fully qualified domain name of the host that needs to be resolved.

Network Interfaces

- The VPN Client cannot establish tunnels over Token Ring. However, it does not conflict with an installed Token Ring interface.
- DELL Docking Station users running the VPN Client on Windows NT may experience bluescreen failures if the latest version of Softex Docking Services has not been installed. The Softex Docking Service utilities are available directly from the DELL Support Web site, <http://search.dell.com/index.asp>. Select the checkbox for the File Library and search for the term “Softex Docking Services”.

Network ICE BlackICE Defender Configuration

Network ICE's BlackICE Defender is a traffic monitoring security product. If you properly configure it, BlackICE Defender can work with the VPN Client. You must configure BlackICE Defender for Trusting, Nervous, or Cautious mode. If you use Nervous or Cautious mode, add the public IP address of the VPN Concentrator to the list of trusted addresses. You can now configure the VPN Client to work with BlackICE Defender configured for Paranoid mode when in Tunnel-everything mode. Split Tunneling requires BlackICE to be in Trusting, Nervous, or Cautious mode.

The Cisco VPN Client firewall has the following requirements for BlackICE (BlackICE Defender 2.5 or greater or BlackICE Agent 2.5 or greater). For BlackICE Defender 2.5, copy the BICTRL.DLL file from the Cisco installation release medium to the BlackICE installation directory on the VPN Client PC. This is a mandatory step for making a connection requiring BlackICE.

BlackICE Defender version 2.9 and greater includes the BICTRL.DLL file in the Network ICE distribution medium, so that you do not need to copy it from the Cisco installation release medium.

Microsoft Outlook Error Occurs on Connection or Disconnect

The following Microsoft Outlook error might occur when the VPN Client connects or disconnects:

“Either there is no default mail client, or the current mail client cannot fulfill the messaging request. Run Microsoft Outlook and set it as the default mail client.”

This message does not affect operation of the VPN Client. The issue occurs when Microsoft Outlook is installed but not configured for email, although it is the default mail client. It is caused by a Registry Key that is set when the user installs Outlook.

To eliminate this message, do one of the following:

- Right-click the Outlook icon, go to Properties, and configure it to use Microsoft Exchange or Internet Mail as the default mail client.
- Use Internet Explorer to configure the system to have no default mail client.
- Configure Outlook as the default mail client (CSCdv67594).

Adjusting the Maximum Transmission Unit (MTU) Value

VPN Encapsulation adds to the overall message length. To avoid refragmentation of packets, the VPN Client must reduce the MTU settings. The default MTU adjusted value is 1300 for all adapters. If the default adjustments are not sufficient, you may experience problems sending and receiving data. To avoid fragmented packets, you can change the MTU size, usually to a lower value than the default. To change the MTU size, use the VPN Client SetMTU utility. If you are using PPPoE, you may also have to set the MTU in other locations. Refer to the following table for the specific procedures for each type of connection.

The MTU is the largest number of bytes a frame can carry, not counting the frame's header and trailer. A frame is a single unit of transportation on the Data Link Layer. It consists of header data, plus data that was passed down from the Network Layer, plus (sometimes) trailer data. An Ethernet frame has an MTU of 1500 bytes, but the actual size of the frame can be up to 1526 bytes (22-byte header, 4-byte CRC trailer).

Recognizing a Potential MTU Problem

If you can connect with the Cisco VPN Client but cannot send or receive data, this is likely an MTU problem. Common failure indications include the following:

- You can receive data, such as mail, but not send it.
- You can send small messages (about 10 lines), but larger ones time out.
- You cannot send attachments in email.

Setting the MTU Value

Usually, an MTU value of 1300 works. If it doesn't, the end user must decrease the value until the Cisco VPN Client passes data. Decrement the MaxFrameSize value by 50 or 100 until it works.

The following table shows how to set the MTU value for each type of connection.

Connection Type	Procedure
Physical Adapters	Use the SetMTU utility supplied with the Cisco VPN Client.
Dial-up	Use the SetMTU utility supplied with the Cisco VPN Client.
PPPoE - All Vendors	Windows XP only Use SetMTU

Connection Type	Procedure
PPPoE - EnterNet	Windows 9x <ul style="list-style-type: none">• On the main desktop, right click on My Network Places and go to Properties. The Network window opens.• Double-click the Network TeleSystems PPPoE Adapter.• On the Network TeleSystems window, click the Advanced tab, and then click MaxFrameSize. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.
	Windows 2000 <ul style="list-style-type: none">• On the main desktop, right-click My Network Places and go to Properties. The Network and Dial-Up Connections window opens.• Right-click and go to Properties on each connection until you find the connection that has the NTS EnterNet PPPoE Adapter.• Once you find the correct connection, click Configure on the right side of the window.• On the next window, click the Advanced tab, then click MaxFrameSize. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.

Connection Type	Procedure
PPPoE - WinPoet	<p>Windows 9x: WinPoet does not provide user control over the PPPoE MTU under Windows 9x.</p> <p>Windows 2000</p> <p>WinPoet does not provide a user interface to control the MTU size, but you can control it by explicitly setting the following registry key:</p> <p>HKLM/system/currentcontrolset/control/class/<guid>/<adapternumber> adapter(000x): Value: MaxFrameSize Value type: DWORD Data: 1300 (or less)</p> <p>The GUID and adapter number can vary on different systems. Browse through the registry, looking for the MaxFrameSize value (CSCdu80463).</p> <div data-bbox="302 735 344 776"></div> <p>Caution Edit the registry only if you are comfortable doing so. Incorrect registry entries can make your PC unstable or unusable.</p>
PPPoE - RasPPPoE	<p>Windows 9x</p> <ul style="list-style-type: none"> On the main desktop, right-click My Network Places and go to Properties. The Network window opens. Find the PPP over Ethernet Protocol that is bound to the Network card that is in your PC, then double click on it. In the General Tab check Override Maximum Transfer Unit. Change the value here. The value varies from case to case. The range can be from 1200 to 1400. <p>Windows 2000</p> <ul style="list-style-type: none"> On the main desktop, right-click My Network Places and go to properties. The Network and Dial-Up Connections window opens. Right-click the connection the PPPoE Protocol was installed to, and go to properties. When the window opens, double-click PPP over Ethernet Protocol. In the General Tab, check Override Maximum Transfer Unit. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.

Asante FR3004 Cable/DSL Routers Require Asante Firmware Version 2.15 or Later

Versions of the Asante firmware caused a problem with rekeying and keepalives when a VPN Client had an all-or-nothing connection to a VPN Concentrator through an Asante FR3004 Cable/DSL router. Version 2.15 (or later) of the Asante firmware resolves these issues. For more information about Asante cable/DSL routers, see the following Web sites:

- <http://www.asante.com/products/routers/index.html>
- http://www.practicallynetworked.com/pg/router_guide_index.asp

Using Nexland Cable/DSL Routers for Multiple Client Connections

All Nexland Pro routers support passing multiple IPSec sessions through to Cisco VPN 3000 Series Concentrators. To enable this function, the Nexland user must select IPSec Type 2SPI-C on the Nexland options page.

The discontinued Nexland ISB2LAN product correctly handles a single connection, but problems can occur when attempting to make multiple client connections to the same Secure Gateway from behind an ISB2LAN Nexland Cable/DSL router. Nexland has fixed this problem in the Nexland Pro series of routers (CSCdt10266).

Cert DN Matching Cannot Match on Email Field EA

You cannot match on the Cert DN field (EA) when using the Peer Cert DN Verification feature because the VPN Concentrator does not assign a value to that field (CSCdx25994).

Long (over 200) Network List Might Cause Client Failure

If the VPN 3000 Concentrator is configured to send a network list containing 200 networks to the VPN Client, the VPN Client service might fail. To resolve this issue, reduce the number of networks in the network list, restart the client PC, and reconnect (CSCdt06772).

VPN Dialer Application Can Load During OS Shutdown or Restart

When using the VPN Client's Start Before Logon feature (Windows NT, Windows 2000, or Windows XP) in "fallback" mode, the VPN dialer application loads during a shutdown or restart of the operating system. This will not cause any problems and can be ignored (CSCdu02071).

America Online Users (AOL) Versions 5.0 and 6.0

The VPN Client supports AOL Version 5.0. AOL Version 6.0 is also supported, with one limitation: when connected, browsing in the network neighborhood is not available.

America Online Users (AOL) Version 7.0

AOL Version 7.0 uses a proprietary heartbeat polling of connected clients. This requires the use of split tunneling to support the polling mechanism. Without split tunneling, AOL disconnects after a period of time between 5 and 30 minutes.

Browser Interoperability Issues

The following known issues might occur when using the VPN Client with the indicated browser software.

Issues Loading Digital Certificate from Microsoft Certificate Store on Windows NT SP5 and on IE 4.0 SP2

The following error occurs in the VPN Client log when using a Digital Certificate from the Microsoft Certificate Store. This can occur on Windows NT 4.0 with Service Pack 5 and on Internet Explorer 4.0 with SP2 and using the VPN Client v3.1 or v3.5:

"Could not load certificate cn=Joe Smith,ou=Engineering,o=MyCompany,l=Buffalo, st=new york,c=US,e=jsmith@mycompany.com from the Unsupported Store store"

Both the VPN Client and the Certificate Manager can see and validate the Certificate, but when you try to connect using that Certificate, you get a message in the Connection History dialog that says, "Failed to establish a secure connection to the security gateway".

To fix this problem, do *one* of the following:

- Upgrade to Internet Explorer v5.0 or greater.
- Upgrade the PC to Service Pack 6.0a (CSCdv70215).

Cannot Connect 3.6 VPN Client for Windows Using Digital Certificate With Non-exportable Keys

A PC must have Internet Explorer version 5.0 SP2 or later installed to function properly using certificates with non-exportable keys (CSCdx90228).

Entrust Entelligence Issues

The following known issues might occur when using Entrust Entelligence software with the VPN Client.

Potential Connection Delay

Using the VPN Client with Entrust Entelligence might result in a delay of approximately 30 seconds if you are trying to connect while Entrust is “online” with the CA. This delay varies, depending on your Entrust CA configuration. If the Entrust CA is on the private network, then the chance of Entrust being online are low, since the VPN connection is needed to communicate with the CA.

If you experience this delay, do *one* of the following:

- Wait for the delay to end and proceed with the VPN connection normally.
- Before initiating the VPN Client connection, log out of Entrust. The VPN Client will initiate the Entrust Login Interface with the “work offline” checkbox checked, which alleviates the problem. The easiest way to log out of Entrust is to right-click on the Entrust tray icon (gold key) and select “Log out of Entrust” (CSCdu25495).

Entrust System Tray Icon Might Erroneously Indicate Logout

When using VPN Client with Start Before Logon (Windows NT and 2000) and Entrust Entelligence, the Entrust system tray icon indicates that it is “logged out” once in Windows. It is really logged in, just not in the normal Windows desktop. The reason for this is that the context that Entrust was logged into was on the “Logon desktop”. This is an Entrust issue, not a VPN Client problem.

Entrust operates normally once logged into within Windows (CSCdu29239).

Entrust Client May Appear Offline

After establishing a VPN connection with Entrust Entelligence certificates, the Entrust client may appear offline. It may appear this way even after the Entrust client has successfully communicated with the Entrust i500 directory.

To work around this issue, do *one* of the following:

- Upgrade to Entrust Entelligence version 5.1 SP3 or later.
- Once connected, right click on the Entrust tray icon (gold key) and uncheck “Work Offline”. This manually puts Entrust online (CSCdu33638).

Use Entrust Entelligence 4.0 with VPN Client Release 3.5.1 or 3.1 Start Before Logon

When using the Release 3.5.1 or 3.1 VPN Client with the Entrust Entelligence 4.0 software, the Start Before Logon feature does not function properly. Upgrading to Entrust Entelligence 5.1 resolves this problem (CSCdu61926).

Some Entrust Dialogs Do Not Display Properly When Using VPN Client Start Before Logon

When using the VPN Client with Start Before Logon and Entrust Entelligence, some Entrust dialogs do not display properly on the logon desktop that displays before going into Windows NT or Windows 2000. The first time the VPN Client dialer and service access the Entrust certificates, it prompts for a security check. This prompt displays in Windows, but not at the logon screen.

To work around this problem, connect the VPN Client once, while in Windows and after installing, to register the VPN applications (ipsecdialer.exe and cvpnd.exe) with Entrust. Once you have done this you can use it at the logon desktop (CSCdu62212).

Renewing Entrust Entelligence Certificate (Key Update) Requires Entrust Version 5.1 SP 3 or Later

Entrust Entelligence certificate renewal (key update) will not work over a VPN Client connection unless Entrust Entelligence version 5.1 SP3 or later is being used. Other Entrust Entelligence operations using older versions work properly.

To work around this issue, do *one* of the following:

- Upgrade to Entrust Entelligence version 5.1 SP3 or later.
- Computers need to have Entrust digital certificates renewed by placing them directly on the network during the renewal period to get updated (CSCdu84038).

Manual Reboot Required after Automatic Uninstall of Nortel VPN Client

If the Nortel VPN Client version 2.51 is upgraded to version 2.62, the Cisco VPN Client detects and offers to uninstall the Nortel Client. After the uninstall completes, the user must manually reboot the PC. Setup does not automatically offer to do the reboot (CSCdu30079).

Accessing Online Glossary Requires Connection to Cisco.com

The Glossary button at the top of all Help screens tries to contact [univercd at www.cisco.com](http://www.cisco.com) (the Cisco documentation site). This connection requires connectivity to Cisco's main web site. If your PC does not have a corporate Internet connection or your firewall blocks access, the following error appears when you attempt to access the Glossary:

“The page cannot be displayed.”

To access the Glossary, you must be connected to www.cisco.com (CSCdy14238).

ZoneAlarm Plus Versions 3.1.274 and Earlier Are Incompatible with VPN Client

The following known incompatibility exists between the Cisco VPN Client and Zone Labs ZoneAlarm Plus version 3.1.274 and earlier. If you are using such a version of ZoneAlarm Plus, please visit <http://www.zonelabs.com> or contact your Zone Labs representative for an update.

On a PC with ZoneAlarm Plus version 3.1.274 (or earlier) and the VPN Client, the following errors occur when the PC boots:

On Windows 2000:

ZAPLUS.exe has generated errors and will be closed by Windows. You will need to restart the program.

An error log is being generated.

The Application Log states:

The application, ZAPLUS.EXE, generated an application error. The error occurred on 7/23/2002... The exception was c0000005 at address 00401881 (<nosymbols>).

Similar errors occur on other Windows operating systems.

The result of this error is that the ZoneAlarm GUI does not run, and therefore a user can not change any settings in ZoneAlarm Plus or allow new programs to access the Internet.(CSCdy16607).

CVPND Listens on UDP Port 500 When Not Connected

When the VPN Client is installed, you will find it is LISTENING on UDP Port 500, which is used for IKE negotiation. Even though the port is in a LISTENING state, the VPN Client cannot accept incoming connection attempts from other IPSec Clients or devices.

The port is in a LISTENING state because the VPN service is started at boot time. This service may take up to 10 seconds to start and if the service was started at connect time, each connection attempt would take an additional 10 seconds to complete. Always having the service running makes call setup time quick for our customers (CSCdt41339).

Harmless Warning Might Occur with Linux Kernel 2.4

Linux users running 2.4 kernels may encounter the following warning when the VPN Client kernel module is loaded:

Warning: loading /lib/modules/2.4.18-3/CiscoVPN/cisco_ipsec will taint the kernel: no license

This message indicates that the VPN Client kernel module is not licensed under the GPL, so the Linux kernel developers will not debug any kernel problems that occur while this kernel module is loaded. This message does not affect the operation of the VPN Client in any way (CSCdy31826).

Open Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. The following lists are sorted by platform and then by identifier number for the specified platform.

**Note**

If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, choose Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats for the VPN Client on Windows Systems

This section lists open caveats for the VPN Client running on a Windows platform.

- CSCdt07491

The VPN Client may swap Primary and Secondary WINS received from the Concentrator. In a few cases, the VPN Client receives a Primary and a Secondary WINS server from the Concentrator but swaps them when they are added to the IP Configuration. If this happens, it may cause browsing problems if the Secondary WINS server is not as populated as the Primary. Disconnecting and reconnecting may fix the problem.

- CSCdt07673

When the VPN Client is installed on a Windows 2000 PC with the Efficient Networks NTS EnterNet 300 PPPoE version 1.41, the following message appears:

“EnterNet could not find the (adapter) for complete pc management NIC (adapter). But it did locate the (adapter) for complete pc management NIC (adapter) - Deterministic Network Enhancer Miniport adapter through which your network server is reachable. Do you want to switch to this adapter?”

Answer Yes every time this question appears. The installation then continues normally.

A similar message appears on Windows NT 4.0. The message is:

“EnterNet could not find the (adapter). But it did locate the (adapter) through which your network server is reachable. Do you want to switch? Yes No”

Answer Yes to this question. The installation then continues normally.

If the VPN Client is uninstalled, the next time the NTS EnterNet 300 PPPoE version 1.41 is used the message, “EnterNet could not find the (adapter). But it did locate the (adapter) through which your network server is reachable. Do you want to switch? Yes No”

Answer Yes to this question. The installation then continues normally.

- CSCdt07787

Problems have occurred when an ISA legacy NIC card (IBM Etherjet 10MB) is used in a PC with PnP OS enabled. The WINS servers did not function correctly when a VPN Client connection was made. This could be an issue with other legacy NIC cards as well.

The end results are that the WINS servers sent from the Secure Gateway cannot be viewed in the Network configuration, and problems with browsing/logon over the VPN connection may occur.

Workaround:

Disable PnP OS in the PC's BIOS or statically configure the WINS servers.

- CSCdt13380

When you connect the VPN Client to a VPN 3000 Concentrator that issues two DNS servers, both appear under ipconfig /all, but only one appears under the Network settings TCP/IP Properties. DNS server appears to be missing under TCP/IP Properties (Advanced button, DNS TAB). We do not know whether this causes any problems.

- CSCdt13398

During a split-tunnel VPN Client connection, the first packets that bring up a new IKE SA may be lost. You may need to reconnect or relaunch network applications that do not automatically try to reconnect on their own.

- CSCdt41308

You may see a problem with FTP file transfers over a long period of time (hours) while connected with the VPN Client. The symptom is that the FTP session never starts (no response to the 'open' command) and the Client Log Viewer shows the following events:

74 22:31:08.704 02/08/01 Sev=Warning/2 IPSEC/0xE370000C
Failed to acquire a TCP control resource, the queue is empty.

75 22:31:08.704 02/08/01 Sev=Warning/2 IPSEC/0xA370001A
VRS processing failed, discarding packet

Other applications like PING and HTTP should work fine, but for FTP to work again, you must disconnect and reconnect the VPN Client.

- CSCdt42661

When using the VPN Client behind an ESP-aware NAT/Firewall, the port on the NAT/Firewall device may be closed due to the VPN Client's keepalive implementation, called DPD (Dead Peer Detection). When a Client is idle, it does not send a keepalive until it sends data and gets no response.

See the description of "Allowing the VPN Client to Work Through ESP-Aware NAT/Firewalls" on page 16 in these Release Notes for more information. Refer to "Connection Profile Configuration Parameters" in the *VPN Client Administrator Guide* for a detailed description of creating profiles.

- CSCdt56343

You might see the following problem on systems running Windows NT and Windows 2000 when you are using the Start Before Logon feature of the VPN Client with third-party dialer. If the third-party dialer does not get set to the foreground when launched, add the following parameter to the vpnclient.ini file in the VPN Client directory (\Program Files\Cisco Systems\VPN Client\Profiles):

```
[main]
TopMostDelay=2500
```

The value is the time in milliseconds that the VPN Client waits for the third party dialer to load before attempting to place it in the foreground. The default time is 1000 milliseconds.

Workaround:

For problem dialers/applications, try 2500 milliseconds or greater.

- CSCdu22174

SCEP enrollment might fail to complete successfully after the PKI administrator has granted your request.

Workaround:

If this happens, delete your failed request and submit a new one.

To delete the request, open the Certificate Manager. Click the Enrollment Requests tab, and highlight the failed request. Select Options and delete.

- CSCdu50445

The following issue can exist when using the VPN Client Start Before Logon feature with Entrust SignOn. Entrust SignOn is an add-on to the Entrust Entelligence client that allows logging into the Entrust profile and the NT domain from a single login.

The Entrust SignOn GINA dll does not support chaining to other GINA dll files. To make the Entrust SignOn product and the VPN Client with Start Before Logon function properly together, install the VPN Client after Entrust SignOn. The VPN Client replaces the Entrust GINA (etabcgina.dll) with its own (csgina.dll).

- CSCdu62275

VPN Client and Entrust Entelligence - VPN Connection Manager timeout.

The potential exists for the VPN Client Connection Manager and the VPN Dialer to get out of sync with each other. This occurs only after a VPN Client upgrade on the first time the VPN Client accesses a given Entrust profile. The following sequence outlines how a user could get the connection into this state:

-
- | | |
|---------------|---|
| Step 1 | In the VPN dialer, the user clicks Connect. |
| Step 2 | Entrust prompts for password and security hash check. The user clicks Yes. |
| Step 3 | Entrust prompts for password for cvpnd.exe security access.

If the user waits here or walks away from PC, the Connection Manager times out in 3 minutes. |
| Step 4 | The user returns and enters the Entrust password, then clicks Yes to the security hash check question. |
| Step 5 | The VPN connection completes, and data can be passed. The VPN dialer appears as not connected. |
| Step 6 | Clicking Connect returns "A connection already exists". The user clicks Cancel, and the dialer appears connected in the system tray. |

The VPN connection can be used as a normal connection.

- CSCdu70660

This issue occurs on a Windows NT PC that is running ZoneAlarm, if the VPN Client is set to Start Before Logon and an upgrade to the VPN Client is implemented. Do not attempt a connection before the logon when you reboot, because ZoneAlarm does not automatically give the VPN Client permission to access the Internet. ZoneAlarm sees the upgrade as a new application attempting to access the Internet, and it requires user permission through its pop-up menus. The user must logon to the Windows NT PC using cached credentials, then launch a VPN connection. ZoneAlarm then asks permission to allow the VPN Client to connect. Answer yes to each connection. After that, Start Before Logon works fine.

- CSCdu77405

The message, “The necessary VPN sub-system is not available. You will not be able to make a connection to the remote IPSec server.” might appear on a PC when Start Before Logon is enabled on the Client and ZoneAlarm is also running. The message appears when the ctrl+alt+del key combination is pressed. This has happened because the Cisco Systems VPN Service has terminated unexpectedly.

Workaround:

Logon to the PC with cached credentials, open “Services” in control panel and start the VPN service. A connection to the VPN Concentrator will be possible once the service has started.

- CSCdu81905

When connecting to a VPN 3000 Concentrator over PPPoE using the EnterNet 300 client software from Efficient Networks, Inc., if a firewall is required by the VPN Concentrator, the following message might appear:

“The Client did not match any of the Concentrator's firewall configurations...”

If this message appears, click OK and then click Connect. The connection to the VPN Concentrator then proceeds successfully.

- CSCdu83054

If you make connections from the command line interface using the NoTrayIcon parameter, the following problem can occur. When a firewall is required to connect and the firewall fails or is shut down, you do not see any message giving the reason for the lost connection.

- CSCdu86399

If you use the VPN Client with a Digital Certificate and your Client sits behind a Cable/DSL router or some other NAT device, you might not be able to connect to your VPN Gateway device (that is, the VPN 3000 Concentrator). The problem is not with the VPN Client or the Gateway; it is with the Cable/DSL router. When the VPN Client uses a Digital Certificate, it sends the Certificate to the VPN Gateway. Most of the time, the packet with the Certificate is too big for a standard Ethernet frame (1500), so it is fragmented. Many Cable/DSL routers do not transmit fragmented packets, so the connection negotiation fails (IKE negotiation).

This problem might *not* occur if the Digital Certificate you are using is small enough, but this is only in rare cases. This fragmentation problem happens with the D-Link DI-704 and many other Cable/DSL routers on the market. We have been in contact with a few of these vendors to try to resolve the issue.

Testing with the VPN Client Release 3.1 indicates that VPN Client connections using Digital Certificates *can* be made using the following Cable/DSL routers with the following firmware:

Linksys BEFSRxx v1.39 or v1.40.1

SMC 7004BR Barricade R1.93e

Nexland Pro400 V1 Rel 3M

NetGear RT314 V3.24(CA.0)

Asante FR3004 V2.15 or later

Others like 3COM 3C510, and D-Link DI-704 either had updated firmware that was tested and failed, or had Beta firmware that was NOT tested because the firmware notes did not indicate a fix specifically for fragmentation.

- CSCdu87521

The following message might appear when a connection using the EnterNet 300 version 1.4 PPPoE software and transferring via FTP:

93 09:42:06.020 08/02/01 Sev=Warning/2 IPSEC/0xE3700002
Function CniInjectSend() failed with an error code of 0xe4510000
(IPSecDrvCB:517)

This does not interfere with your connection. You can ignore this message.

- CSCdv40009

When Zone Alarm's Internet setting is set to high and the VPN Concentrator sends a CPP firewall policy that allows inbound traffic on a specific port, the CPP rule takes precedence over the Zone Alarm rule allowing the specified port to be open.

- CSCdv42414

Importing a PKCS12 (*.p12 or *.pfx) certificate using the Certificate Manager that has not been password protected will fail with the following error:

“Please make sure your import password and your certificate protection password (if for file based enrollment) are correct and try again.”

Workaround:

Get a *.p12 certificate that has been password protected.

- CSCdv43347

If the Cisco VPN Client is not connecting when configured for digital certificates, the problem may not be indicated on the VPN Client connection history dialog. It may be helpful to run the Log Viewer application to see if any events are being displayed. To load it, click on the following and retry the connection.

Start->Programs->Cisco Systems->VPN Client->Log Viewer

- CSCdv44529

Attempting to install/uninstall Gemplus Workstation version 2.x or earlier while the Cisco VPN Client and its GINA (csgina.dll) is installed will cause the following error, and Gemplus will not install/uninstall:

“A 3rd party GINA has been detected on your system. Please uninstall it before installing this product.”

Workaround:

Do *one* of the following:

- Uninstall the VPN Client and reinstall it after Gemplus software.

or

- Use Gemplus version 3.0.30 that no longer installs the gemgina.dll

- CSCdv46591

When a CPP Firewall policy is in place that drops all inbound and outbound traffic and no WINS address is sent to the VPN Client from the 3000 series Concentrator, Start Before Logon fails. If a WINS address is in place, Start Before Logon works fine. Also, if a WINS address is sent and the CPP rule drops all inbound traffic, but allows all outbound traffic, Start Before Logon works fine.

- CSCdv46937

Using the Aladdin “R2” model etoken, certain functions can be performed using the certificate even after the R2 token has been detached from the system (USB port). The VPN Client, for instance, can perform an IKE rekey without the token attached to the system. The reason for this is the design of the “R2” etoken: it does not contain the RSA key functions needed and must upload the private key to the system for these functions.

In contrast, the Aladdin “PRO” etoken must be connected to the USB port during an IKE rekey, otherwise the VPN Client connection terminates. This is Aladdin’s problem; it is not a VPN Client problem.

- CSCdv62613

When you have multiple VPN Client connections behind Linksys Cable/DSL router, the following problem can occur. Due to a Linksys problem with firmware versions 1.39 and 1.40.1, making multiple VPN Client connections enabling the feature “Allow IPSec over UDP” (transparent tunneling) may cause data transfer problems.

Allow IPSec over UDP is a VPN Client feature that allows ESP packets to be encapsulated in UDP packets so they traverse firewall and NAT/PAT devices. Some or all of the clients may not be able to send data. This is due to a Linksys port mapping problem, that Linksys has been notified of.

Workaround:

If possible, do not use the “Allow IPSec over UDP” (transparent tunneling) feature when you have multiple VPN Client connections behind Linksys Cable/DSL router.

- CSCdv67594

The following Microsoft Outlook error might occur when the VPN Client connects or disconnects. This occurs when Microsoft Outlook is installed but not configured.

In Microsoft Outlook, either there is no default mail client or the current mail client cannot fulfill the messaging request. Run Microsoft Outlook and set it as the default mail client.

To do this, right-click on the Outlook icon, go to Properties, and configure it to use Microsoft Exchange or Internet Mail.

- CSCdv85740

Using BlackICE Defender version 2.9 with Windows 95 might cause a reboot or a blue screen after the connection to the Concentrator has been active for a period of time. This is a problem with NetworkICE, not the VPN Client.

- CSCdw60866

Getting Entrust certificates using SCEP does not get the Root CA certificate. The Entrust CA does not send the whole certificate chain when enrolling with SCEP. Therefore, making a VPN Client connection might require the manual installation of the Root certificate before or after SCEP enrollment. Without the existence of the Root CA certificate, the VPN Client fails to validate the certificate and fails with the following VPN Client event/error messages:

“Get certificate validity failed”

“System Error: Unable to perform validation of certificate
<certificate_name>.”

- CSCdw73886

If an attempt to load the VPN Client is made before the Clients Service loads, the following error occurs: “The necessary VPN sub-system is not available. You will not be able to make a connection to the remote IPSec server.”

Workaround:

Wait until the Service has loaded, then start the VPN Client.

- CSCdx45719

Downgrading the Cisco VPN Client from 3.6 to 3.5 and using the Start Before Logon feature results in the Start Before Logon running in fallback mode. This is due to some enhancements made to the csgina.dll file in 3.6 that the 3.5 VPN Client does not implement.

Workaround:

If downgrading and Start Before Logon are necessary, manually remove the VPN Client and then delete the csgina.dll file in the systems directory (usually c:\winnt\system32). This allows the 3.5 VPN Client to install its own csgina.dll file and operate normally.

- CSCdx51632

If the computer is powered off or loses power during an MSI installation of the VPN Client, the VPN Client may not be registered in Control Panel, and the following may occur when attempting to reinstall:

- A message may appear stating:
Deterministic Network Enhancer Add Plugin Failed
Click the “OK” button.
- Error 1722. There is a problem with this Windows Installer package. A program as part of the setup did not finish as expected. Contact your Support personnel or package vendor. Click the “OK” button.
- Error 1101. Error reading from file c:\config.msi\laff4.rbs. Verify that the file exists and you can access it. Click the “OK” button.
- Error 1712. One or more of the files required to restore your computer to its previous state could not be found. Restoration is not possible. Click the “OK” button.

After clearing the last message box, restart MSI installation. It should successfully install the VPN Client.

- CSCdx72463

Installing the VPN Client using the Microsoft Windows Installer (MSI) displays “Time Remaining” for the installation. This time is not very accurate and should be ignored.

- CSCdx77292

Microsoft article Q234859 states that for the resiliency feature to work on Windows 4.0, IE 4.01 sp1 and shell32.dll version 4.72.3110.0 or greater must be installed on the computer.

- CSCdx78868

The Microsoft Installer (MSI) resiliency (self healing) feature does not restore all files that are installed with the VPN Client. The files that will be restored are files that are associated with the shortcuts under Start | Program Files | Cisco Systems VPN Client.

- CSCdx81491

An issue can occur when using the 3.6 VPN Client with Start Before Logon (SBL), after enabling SBL. The first time you log out of Windows, the VPN Client does not load after you press the CTRL+ALT+DEL key combination at the Windows logon prompt.

Workaround

Reboot the PC after enabling Start Before Logon; after a subsequent logout, the VPN Client should operate properly.

- CSCdx83687

The following error occurs after the resiliency feature has reinstalled a missing file on Windows NT 4.0:

```
c:\winnt\profiles\all users\start menu\programs\cisco systems  
vpnclient\xxx.lnk
```

The Windows installer failed to install the program associated with this file.

Please contact your system administrator.

xxx.lnk is whatever file is being restored.

When you click OK, the PC reboots and the file *is* restored. The resiliency feature is working, but the error should not appear.

- CSCdx88063

When attempting to launch the dialer when the dialer is already running on the logon desktop (due to SBL or SBL and AI), the following error occurs instead of the VPN Client dialer loading.

“Single dialer instance event creation failed with error 5.”

This is most likely to happen when Start Before Logon and Auto Initiate are being used on a Windows NT/2000/XP system.

Workaround

This is due to the fact that the VPN Client dialer is already running on the “logon desktop”. Most likely during Windows logon the dialer launched and posted an error, the Windows logon was completed and the error was never closed. To work around this error, do the following:

-
- | | |
|---------------|---|
| Step 1 | Press CTRL+ALT+DEL to get to the logon desktop. |
| Step 2 | Look for and close any VPN Client error dialogs. |
| Step 3 | Press ESC to return to the normal Windows desktop; the VPN Client should load normally. |
-

- CSCdx89940

A Restricted, Standard, or Limited user (Windows 2000) cannot install the VPN Client using the Windows Installer (MSI), even if elevated privileges are set for the user and the PC.

- CSCdy13425

Connecting the Cisco VPN Client (versions 3.5 and later) to an IOS VPN device running 12.2(8)T using digital certificates might disconnect during a rekey. The connection could disconnect sooner if dead peer detection (DPD) is being used. The problem is under investigation.

Workaround:

Keeping the rekey times as high as possible will help avoid the problem.

The other alternative is to use the VPN Client with preshared keys, which does not have the problem.

- CSCdy14218

During installation of the VPN Client on a PC that already has the Enternet v.1.5c or v. 1.5c SP2, the following error might appear:

“SVCHOST.EXE has generated errors and will be closed by Windows.”

Workaround:

If this message appears, click OK, then reboot the PC when the VPN Client prompts for the reboot. After this, The message does not reappear and all connections work fine.

- CSCdy47745

In the following specific case, the VPN Client fails to sent its IKE Keepalives (DPD - Dead Peer Detection) and then disconnect after the VPN Concentrator has been rebooted. This occurs only in the case where the VPN Client has been receiving the following Events in its log (also see [CSCdt41308](#)):

```
421      12:32:17.981  08/28/02  Sev=Warning/2 IPSEC/0xA3700019
VRS processing failed, discarding packet
```

```
422      12:32:19.984  08/28/02  Sev=Warning/2 IPSEC/0xE370000B
Failed to acquire a TCP control resource, the queue is empty.
```

Open Caveat for Linux

This section lists the open caveat for the VPN Client running on a Linux platform.

- CSCdv73541

The make module process fails during installation of the VPN Client.

Workaround:

The module build process must use the same configuration information as your running kernel. To work around this problem, do one of the following:

- If you are running the kernels from Red Hat, you must install the corresponding kernel-sources rpm. On a Red Hat system with kernel-sources installed, there is a symlink from `/lib/modules/2.4.2-2/build` to the source directory. The VPN Client looks for this link first, and it should appear as the default value at the kernel source prompt.
- If you are running your own kernel, you must use the build tree from the running kernel to build the VPN Client. Merely unpacking the source code for the version of the kernel you are running is insufficient.

Open Caveat for Solaris

This section lists the open caveat for the VPN Client running on a Solaris platform.

- CSCdv75825

If the VPN Client uses routed RIP to learn its default route, you might lose connectivity. This is because RIP is blocked when the VPN Client is connected in all tunneling mode.

Open Caveats for Mac OS X

There are no open caveats for the VPN Client running on Mac OS X.

Caveats Resolved in Release 3.6.5

Release 3.6.5 resolves the following issues:

- CSCeb42091

Cisco VPN Service (cvpnd.exe) crashes when the service is stopped. This happens only on windows XP. This is a very rare occurrence. This was reported by a third party and happened only in their environment. The service had no problem restarting.

- CSCeb37488

When specifying a third-party dialer in a VPN Client connection profile, if arguments are used (such as profile name to dial) with quotes, they are not parsed correctly and the connection might fail.

For example:

```
c:\winnt\system32\rasphone.exe -d "Some Dialer"
```

This resulted in the VPN Client launching the dialer, but once the dialup connection was complete, the VPN Client would not continue on with the IPsec connection; it simply stayed at the "Initiating remote access connection to your ISP, please wait" message. The VPN Client's log contains the following PPP event message after the failure: Invalid command "B"

Caveats Resolved in Release 3.6.4.A

Release 3.6.4.A resolves the following issues:

- CSCdy79595

Installation of the VPN Client 3.7 on windows XP results in the following error:

"Error: Dneinst execution error while installing DNE, returncode - 2146500093"

- CSCea22263

If the certificate which is to be used by the VPN Client, contains the non-ascii characters in the CN and Subject (letters with umlaut, various kinds of accents, copyright character), then after selecting the certificate in the VPN dialer, closing the VPN dialer, and reopening the same connection entry, there is an error message, "The certificate <name>, associated with this Connection Entry, no longer exists. Please select another certificate."

In the certificate list, though, this certificate is still present and can be selected.

- CSCdz36304

During the VPN Client installation on Windows XP builds after XP Beta 2, an error message appears *behind* the VPN Client installation window that says:

The software you are installing for this hardware:

Deterministic Networks Enhancer Miniport

has not passed Windows Logo testing to verify its compatibility with Windows XP.

You are allowed to "Continue anyway" but this message pops up a few more times after this. Select "Continue anyways" until it stops prompting you (can be as many as 24 times!) and the installation will continue normally.

If you go into the Control Panel | System Hardware | Driver Signing and set XP "Driver Signing" to Ignore, when you install the Client, you do not see any of these messages.

Caveats Resolved in Release 3.6.4

Release 3.6.4 resolves the following issues:

- CSCdx89940

A Restricted, Standard, or Limited user (Windows 2000 or XP) cannot install the VPN Client using the Windows Installer (MSI), even if elevated privileges are set for the user and the PC. The user must have administrative privileges to install the VPN Client.

- CSCdy54329

Installing the Release 3.6 VPN Client on a Windows XP system that has Service Pack 1 applied might result in a Hardware Installation warning that the Deterministic Network Enhancer Miniport drivers are not signed. The installation can proceed without complication if you click “Continue Anyway” at all of the warnings. Multiple warnings occur, the number of warnings depending on the system configuration.

For background information about this issue, see the Microsoft Knowledge Base article number MS02-050 at the following URL:

<http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS02-050.asp>

One of the MS CA Certificates does not contain the appropriate CA extensions and once the patch is applied, it was considered invalid and resulted in all drivers signed underneath it to be considered invalid.

- CSCdy65549

If a user installs the VPN Client and is not a local administrator, but is a domain user that has been added to the local administrator group, the install completes successfully, but you may get the error “VPN subsystem unavailable” when trying to use the client, and you cannot use the client.

If the user installing the VPN Client is a local administrator, then no error is received when running the VPN Client.

- CSCdz38865

When installing Release 3.5.3 and later, up to Release 3.6.3 of the VPN Client on a Dell C810 with the integrated Truemobile card, the following error occurs:

Installation error. Windows has encountered errors while trying to run DNE.exe.

Program will be closed.

The VPN Client still appears to install correctly, but when starting the application, the following error reads:

The necessary VPN sub-system is not available. You cannot connect to the remote VPN server.

- CSCdz51629

When using a Siera SMC2632W wireless card, and building a VPN tunnel to a PIX firewall using split-tunneling, then no SA's are built for the networks in the split-tunnel list, resulting in no traffic flow over the tunnel.

- CSCdz83065

When using the Microsoft Installer (MSI) to uninstall the VPN Client, MSI does not detect that the VPN Client is connected, and the uninstall completes. We highly recommend you disconnect and exit the VPN Client before uninstalling.

Caveats Resolved in Release 3.6.3.C

Release 3.6.3.C resolves the following issues:

- CSCdz85778

The CVPND service might fail under the following conditions: a VPN Client connection is up, Zone Alarm *or* Sygate Personal FW is required, Stateful Firewall is enabled, and the required firewall service is stopped. The failure occurs when AYT disconnects the VPN Client because the required firewall is no longer running.

- CSCea05185

The InstallShield version of the Release 3.6.x VPN Client, as well as 3.6 versions, do *not* detect an existing Cisco IT 3.5(A) VPN Client installed on the PC. It installs the new version on top of old one. The VPN Client *requires* the old version to be uninstalled first; otherwise the new installation may not properly update required files.

Cisco employees *must* first check to see if whether the Cisco IT 3.5(A) version of the VPN Client is installed and must manually unistall it before installing the Release 3.6 VPN Client.

- CSCea16542

When using Windows XP with VPN Client Releases 3.6.3 and 3.6.3.B over a broadband connection, DNS entries are not passed down to a user from mode-cfg. The VPN 3030 Concentrator logs the show the correct DNS sever IPs being sent, and the VPN Client log shows the correct DNS server IPs being recieved without error; but these are not being pushed down to the VPN Client. The same user recieves and uses the correct DNS server IPs with a dialup connection.

- CSCea29015

A Windows NT 4.0, Windows 2000, or Windows XP machine blue screens at address nt!IoVCompleteRequest+0x12c in certain edge cases.

- CSCea31386

After an existing connection is disconnected because the remote peer is not responding, the VPN Client tries to connect to the backup server. This is a problem only after the connection has been established, and the remote peer stops responding for some reason. We should not try to connect to the backup if the existing connection goes down.

Caveats Resolved in Release 3.6.3.B

Release 3.6.3.B resolves the following issues:

- CSCdv43347

If the Cisco VPN Client is not connecting when configured for digital certificates, the problem may not be indicated on the client connection history dialog. It may be helpful to run the Log Viewer application to see if any events are being displayed. To load it, retry the connection by clicking the following path:

Start > Programs > Cisco Systems > VPN Client > Log Viewer

- CSCdw61796

The Cisco VPN Client fails to connect while configured for digital certificates and posts the following error in the Log Viewer:

“Get certificate validity failed”.

Some of the reasons this event could have occurred should be posted to Connection Status dialog and the Log Viewer. We notify the user with the following errors:

- The certificate has an incomplete chain.
 - The certificate is either expired or not valid yet.
 - Certificate private key could not be opened.
 - Certificate signature was invalid.
 - User Certificate was not found.
 - Out of memory
- CSCdx54679
- When a Cisco VPN Connection is not established, users can't get to servers on the private network. But the Novell client caches these negative responses for performance reasons. But when a VPN Connection comes up, Novell client does not know that it can now reach the private servers, and fails the attempt to reach the private server (based on its cache). This can take users up to 5 minutes to reach the private Novell servers.

For Novell client symptoms, see:

<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10068795.htm>.

To avoid this problem, the Cisco VPN Client notifies the Novell driver after the VPN Connection comes up. Novell then clears its cache as a result of this notification. To avoid synchronization issues, we only notify the Novell client 5 seconds after the VPN Tunnel has come up.

- CSCdx70204
- When a profile is copied/clone, any GUI locked parameters are lost in the copied profile.
- CSCdy50212
- When PC with VPN Client, Release 3.6 has the outside interface of the concentrator as its default gateway, the default gateway will be removed out of the windows routing table when the client disconnects. This has been seen only with non-English versions of Windows 2000 Professional and Windows 98SE.

- CSCdy62416

The VPN Client does not establish a connection using digital certificate to the central-site concentrator when behind a NAT device that prevents or corrupts IP fragments.

- CSCdy66378

On some laptops, when using an onboard Ethernet card, the DNS server information that is pushed down through mode config is not used. Using a PCMCIA adapter on the same laptop works fine.

- CSCdy81064

When the adapter address changes, we disconnect the VPN Connection. But the only message in the log states:

```
111 13:58:38.601 10/03/02 Sev=Info/4 CM/0x6310001F
Adapter address changed. Terminate secure connections
```

We should have better log messages to debug this problem. The old message was removed, and the following two new messages were added.

When the connection is established, we display the log message:

```
Address watch added for 10.10.10.10. Current addresses are
10.10.10.10,10.10.10.12.
```

From the above message we know that the address used to establish the connection was 10.10.10.10. We also know that the system has two IP Addresses - 10.10.10.10, and 10.10.10.12.

If the address 10.10.10.10 changes, we will disconnect the connection, and log the following message:

```
Adapter address changed from 10.10.10.10. Current addresses are
10.10.10.12, 10.10.10.13.
```

- CSCdz23365

The installation instructions at the following URL are incorrect if you are installing the VPN Client in fallback mode:

http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_administration_guide_chapter09186a00800bd991.html#xtocid10

IF MSGINA.DLL is the only GINA installed, then a line in the vpnclient.ini that says:

```
INCOMPATIBLEGINAS=MSGINA.DLL
```

does not make the client install in fallback mode, even if the GINA is also specified in the registry as being the GINA that is installed.

- CSCdz26371

In a setup where a VPN Client is behind a natted device and connects to a VPN 3000 Concentrator using NAT-T (NAT Traversal), the Concentrator may think its behind a natted device as well and send keepalive packets to the VPN Client on destination port UDP 4500.

The NAT-T feature helps devices determine whether NAT exists between IKE peers as well as where the NAT is. This information is negotiated in NAT-T payload. A VPN Client behind a natted device might fool the Concentrator into thinking that it is also behind a nat device. This might cause the Concentrator to send keepalive packets, which might get dropped by the NAT device on the VPN Client side.

- CSCdz27476

In certain conditions, the FQDN retrieved from the certificate sent by the headend, may not be retrieved correctly, therefore causing the failure of phase 1:

```
38 13:26:00.104 11/11/02 Sev=Warning/3 IKE/0xE3000081
```

```
Invalid remote certificate id: ID_FQDN: ID = headend.fqdn, Certificate
= headend.fqdn@
```

Where "@" is a printable character (in this case the difference will be seen immediately), or a non-printable character (in this case the FQDNs are seemingly the same).

- CSCdz32947

After installing version 3.6.x VPN Client and enabling stateful firewall, the machine fails with a blue screen. This event occurs only when stateful firewall is enabled.

- CSCdz41646

The connection dialog should show the certificate name during the connection establishment. This lets the user know which certificate is being used to establish the VPN Connection.

- CSCdz49381

Installing the VPN Client from a network drive momentarily disconnects network drives and can cause the installation to fail.

To work around this problem, copy the installation files to a local drive and restart the installation.

- CSCdz56951

General Packet Radio Service (GPRS) dialup environments require multiple VPN Client attempts for the tunnel to establish. The reasoning behind this is that as soon as VPN client receives an IP address from the GPRS RAS, it immediately attempts the IKE phase of the tunnel. However, having received an IP address from the RAS doesn't necessarily mean the GPRS link is operational. Therefore the 1st tunnel establishment fails and requires usually a 2nd attempt to establish the tunnel.

Resolution:

Our normal behavior is to dial the RAS connection and then go to the next phase, which is IKE negotiations. But to resolve this issue, we will dial the RAS connection and then wait few seconds (user configured) before starting the IKE negotiations.

The default behavior of the VPN Client remains unchanged. But if users want to wait after dialing the RAS connection, they can do that by modifying the vpnclient.ini file. This file is located in the installation directory (generally "C:\Program Files\Cisco Systems\VPN Client"). Users will have to add another parameter under main as follows:

```
[main]
DialupWait=x
```

where x is in seconds. The default value is 0 seconds. If we do wait, the following info message is logged to the log viewer:

"Waiting x seconds per user request"

This wait would happen if the VPN Client is used to dial the connection, or if the VPN GUI is used to configure a third-party dialer for dialing the connection.

- CSCdz59405

Attempting to uninstall the VPN Client installed with InstallShield might cause the following error message: Error Number: 0x80040703

This indicates that the uninstall program failed to find dll function: InstHelper.IsRasConnectionActive

- CSCdz61884

When setting up an IPSec tunnel with the VPNClient using the CLI parameter “notrayicon”, the tunnel established indicator in the Windows 2000 machine’s registry is not cleared after the tunnel has been terminated or timed out.

- CSCdz62411

The VPN Client does not show the session as disconnected after the session is terminated from the VPN 3000 Concentrator.

- CSCdz72657

It takes too long to establish the tunnel from a windows machine. Users would see that VPN connection hang for couple of seconds at “Contacting the gateway at a.b.c.d”.

This would occur only if XAuth is used for authentication. The Log Viewer would show a long delay between the following 2 messages:

```
209 16:15:21.370 01/30/03 Sev=Info/4CM/0x63100015
```

Launch XAuth application

```
210 16:16:23.683 01/30/03 Sev=Info/4CM/0x63100017
```

XAuth application returned

Remember that the difference between the two messages above also represents the time users take to enter the password in the XAuth dialog box.

This should happen only intermittently.

Caveats Resolved in Release 3.6.3

Release 3.6.3 resolves the following issues:

- CSCdy69001

The VPN client 3.6.1 might cause a Windows BlueScreen critical error. This problem results from incorrect processing by the VPN Client of a return DDNS packet from a DNS server that does not implement DDNS.

If this problem is encountered, cvpndrv.sys (Cisco VPN Driver) would cause the blue screen. If some other driver is causing the blue screen, then more than likely you are encountering some other bug.

- CSCdy77156

With the MSI installer, you need to use the VPNCLIENT_EN.EXE file to update the MSI version. Running this executable does not function properly if you need to use a MSI transform.

- CSCdy86051

TunnelEstablished registry value is supposed to reflect the state of the tunnel.

The following problem was seen on Win XP with VPN Client v3.5 and v3.6.1:

When you close windows during a VPN connection, the VPN Client doesn't change the TunnelEstablished value in reg.base from 1 to 0 during the windows "shut down". And when you then restart Windows the reg.base still says TunnelEstablished value = 1 even though the VPN is not established.

- CSCdz13444

Connection attempts using a VPN Client for Mac OS X fail when the VPN Concentrator is configured for load balancing.

This condition appears only when the VPN Client is attempting to connect using TCP NAT (TunnelingMode=1). This issue was introduced in version 3.6.2 Rel and had been working in previous versions. However, Mac OS X 10.2.x does not allow TCP NAT connections in previous versions and is limited in which interfaces are functional in earlier versions. Mac OS X 10.1.x is fully functional in earlier versions supporting Mac OS X.

Caveats Resolved in Release 3.6.2.B

- CSCdy39938

Split-DNS servername is not released by VPN Client version 3.6 on Windows NT after disconnecting from VPN.

- CSCdy54329

Installing the 3.6 VPN Client on a Windows XP system that has Service Pack 1 applied may result in a Hardware Installation warning that the Deterministic Network Enhancer Miniport drivers are not signed. The installation can proceed without complication by clicking "Continue Anyway" at all of the warnings. There will be multiple warnings, the number will vary depending on the system configuration.

- CSCdy78142

In the v3.x VPN Client, the VPN Client always fails reauthentication after "New PIN mode" when using SDI SoftID software. The problem occurs because the VPN Client always uses the current tokencode with the new PIN when it should be using the next tokencode with the new PIN.

- CSCdy81700

Unable to pass external (non-tunneled) traffic other than ICMP with split tunneling enabled on Mac OSX 10.2.x while connected with the VPN Client. Ping, nslookup, and traceroute still work to external addresses.

The issue will not manifest over wireless or PPP. It is an issue with the checksum negotiated with the hardware of the newer platform hardware. The problem will not be seen on older platforms such as original iMacs.

Caveats Resolved in Release 3.6.2.A

- CSCdy29594

If you are using Windows NT4 and the VPN Client and you connect to your ISP with the Multiple Line feature in the Dial-Up entry, for example to get up a multilink for ISDN, only one line gets connected when initiated from the VPN Client. Dialing from the Dial-Up program in Windows NT works fine.

- CSCdy49082

The latest Red Hat beta release (code-named "null") will be based on the gcc 3.2 compiler, and kernel modules compiled with gcc 2.9x will not work with the kernel in this new release. Since the vpnclient distribution does not include all of the source for the vpnclient kernel module and for existing releases the binary portion of the kernel module is compiled with gcc 2.95.3, existing releases will not work on a gcc 3.2 based system.

- CSCdy61356

When we try to use the Start Before Logon feature with the VPN Client 3.6.1 after bringing up the VPN connection and logging onto the network, we see an error “PPPTool.exe has generated errors and will be closed by Windows.”

- CSCdy67438

In the InstallShield Script file, we were trying to register the gina before we copied the vpnclient.ini file to the installed directory. Moved the copying of the INI files from routine UpgradeProfiles to routine OnFirstUIAfter before we made the call to routine SetupRegistry. This allowed the Gina registration process to obtain the information from the vpnclient.ini file before it registers the gina.

- CSCdy74287

The v3.6.1.Rel VPN Client installation application does not appear to use the IncompatibleGinas line from the VPNCLIENT.INI file and will replace an “incompatible” GINA with the VPN Client GINA, csgina.dll. This will only occur at install time if the .INI file contains the RunAtLogon=1 line.

- CSCdy76318

A new installation of the Linux VPN Client v3.6.2 does not compile because of missing files. After the v3.6.1 VPN Client release, changes to the installation caused a problem in the Linux VPN Client. This issue is not easily apparent when overwriting a previous version of the client.

Caveats Resolved in Release 3.6.2

- CSCdy48192

IPSec over TCP (cTCP) does not work with Release 3.6 or 3.6.1 of the Cisco VPN Client when running on Mac OS X 10.2.

- CSCdy51818

While attempting to use a VPN Client 3.6 on a Mac OS X 10.2 Jaguar platform, Split Tunneling does not work. This only happens on the Mac OS X 10.2 platform. Mac OS X 10.1 performs appropriately.

- CSCdy55145

The VPN Client sometimes sees DPD replies from the VPN Concentrator coming from reversed Public IP address from what the VPN Concentrator has. Issue goes away on its own and doesn't seem to cause disconnects.

- CSCdy59183

The VPN Client with MacOS X 10.2 may fail to connect with the following error message, even when the kernel module is known to be loaded (verified with the "sudo kextstat" command):

"Could not attach to driver. Is kernel module loaded?"

This occurs on VPN Client 3.6.1 on MacOS X 10.2 with IPv6 enabled, and multiple network interfaces enabled.

Caveats Resolved in Release 3.6.1

This section lists the caveats fixed since Release 3.6. If you have an account on CCO you can check the status of any caveat by using Bug Navigator II.

To reach Bug Navigator II on CCO, choose Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl



Note

Release 3.6.1 addresses multiple vulnerabilities for the VPN 3000 Series Concentrators and VPN 3002 Hardware Client. Please refer to the following URL for the details on the vulnerabilities addressed.

<http://www.cisco.com/warp/public/707/vpnclient-multiple2-vuln-pub.shtml>

- CSCdy14510

On Windows 2000 machines with SMS 2.0 client installed and the Cisco VPN Client 3.5.2A set for Start Before Logon, when VPN Client tries to initiate the connection, the VPN Client hangs at "Initializing connection to your ISP".

- CSCdy28446

When installing the VPN Client using a silent MSI install, the VPN Client does not detect if there is no TCP/IP stack installed. The VPN Client requires TCP/IP and will not function without it. If you do perform a silent install on a PC with no TCP/IP stack, after the install completes and reboots, you see the following error when you attempt to run the VPN Client:

Cisco Systems VPN Client

Windows Sockets initialization failed.

- CSCdy36987

When a VPN tunnel is established, the Release 3.6 VPN Client may incorrectly send DNS queries to your ISP's DNS server instead of to your private DNS server. This results in failed attempts to connect to FTP, Telnet, or other servers when attempting connections by DNS name. Connecting by IP Address works fine.

This has been seen only with Windows XP and Dial-Up networking connections.

- CSCdy41127

The VPN Client V3.6 does not work on interface en1 (Apple AirPort WiFi) card when running Macintosh OS X 10.2

Caveats Resolved in Release 3.6

This section lists the caveats fixed since Release 3.5.2.

- CSCdt00735

Certificate Manager: Entrust VPN Connector displays an MD5 and SHA1 Fingerprint verification for a File-based certificate request from VPN Client. The VPN Client currently does not display this Fingerprint in the request.

- CSCdu20804

One of the following error messages might occur when using the Release 3.5.1, 3.1, or 3.0 VPN Client on Windows NT or Windows 2000 with the Start Before Logon feature. After you establish the Client connection and then attempt to logon to the network, you might see one of the following errors messages:

- “A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on may not be available.” This means that you are logged in at the desktop, and you can see network drives and browse the network.
- “The system cannot log you on now because the domain YOURDOMAIN is not available.” This happens less often, but you can't log in at all.

At present, the only way to prevent these errors is to establish the VPN connection, then wait up to 1 minute before attempting the network logon.

- CSCdu36579

When Outlook Express is set to Work Offline mode and you attempt to synchronize any folder with your home Exchange server, synchronization fails on any folder that has changes. It is successful on any folder that is already synchronized. Outlook reports a generic Network Error for each folder that fails.

Cisco VPN Client NATs the IP Address of the host machine it is installed on. But the communication between MS Exchange to MS Outlook is not NAT-compatible. However, any communication initiated by Outlook (for Exchange) has no problem. Only the connections initiated by Exchange (for Outlook) have problems. Any time a new mail arrives on Exchange server, it sends a notification to Outlook. Since this communication is not NAT-compatible, it is dropped. As a result of this, the Outlook client is not notified of any new mail until it contacts the Exchange server. Outlook contacts the Exchange server anytime the user makes any modifications, such as switching folders, sending mail, clicking the “Send/Receive” button etc

To overcome this problem, Microsoft advises disabling Exchange-to-Outlook notifications by updating MAPI property called PR_DISABLE_WINSOCK. This forces Outlook to poll the Exchange server every 60 seconds.

Microsoft identified a problem in MS Outlook 2000 as the cause of this issue. If Outlook is polling and synchronizing at the same time, Outlook hangs. Microsoft said that this problem is fixed in Outlook 2002. Since the fix for this problem was very complicated, Microsoft is not planning on back-porting the fix to Outlook 2000.

To remedy this problem, we provide the users with an option to enable or disable Outlook to Exchange polling. The default behavior is to enable Outlook to Exchange polling. If you prefer synchronization over “new mail notifications”, you can override the default behavior by adding the following variable in vpnclient.ini file (present in the client installation directory):

```
[main]
OutlookNotify=1
```

The IPsec Dialer (or CLI) defaults to polling if this variable is not present or if its value is 0.

- CSCdu57246

A mechanism is needed to allow removal of a pre-defined IncompatibleGina.

Currently, no method exists to remove a GINA from the predefined IncompatibleGinas list that ships with a VPN Client, even though the vendor has fixed the GINA and the customer now wants to use it in non-FallBack mode with the Client. No workaround currently exists.

- CSCdu61922

If ZoneAlarm is uninstalled on a Windows 98, Windows ME, Windows NT 4 or Windows 2000 PC, then reinstalled, after rebooting the PC and launching the VPN Client, the following message might appear:

“The VPN subsystem is not available. A connection to the concentrator will not be possible.”

Click OK, then click Connect on the VPN Client; the connection continues normally.

- CSCdu80463

Transferring large files fails when using a VPN Client connection over a DSL/PPPoE connection. For example, if you use FTP to try to PUT a large file, it stalls and never completes. FTP GETs seem to be OK.

This problem has been seen on Win 2000 using the Verizon DSL software (WinPoET) and Windows XP RC1 using the native PPPoE adapter. There have also been reports that this problem also occurs with NTS EnterNet PPPoE software.

Workaround:

For WindRiver WinPoET and NTS EnterNet, the following workaround is available.

- *For systems other than Windows XP*, modify the MTU on the PPPoE adapter by explicitly changing or creating the following registry key:

```
HKLM/system/currentcontrolset/control/class/<guid>/<adapter number>
```

```
adapter(000x):
```

```
Value: MaxFrameSize
```

```
Value type: DWORD
```

```
Data: 1400 (or less - you may need to experiment)
```

- *For Windows XP*, the SetMTU utility does this function automatically.



Caution

Edit the registry only if you are comfortable doing so. Incorrect registry entries can make your PC unstable or unusable.

- CSCdv11350

If you install a new Network Interface Card (NIC) on Windows 2000 or XP after the VPN Client is installed, the VPN Client starts to connect and complete user authentication, but it then appears stuck at “Securing Communications Channel...”. When this happens, these events appear in the Event Log:

```
35 13:35:02.549 08/17/01 Sev=Warning/3 IKE/0xE300006D
```

```
Cannot match Policy Entry:
```

```
local host=IP ADDR=0.0.0.0, lcl_port = 0
```

```
remote host=IP ADDR=0.0.0.0, dst_port = 0
```

```
36 13:35:02.549 08/17/01 Sev=Warning/3 IKE/0xA3000001
```

```
Failed to initiate negotiation.
```

```
37 13:35:02.549 08/17/01 Sev=Warning/3 IKE/0xE3000002
```

```
Function initialize_qm failed with an error code of 0x00000000  
(INITIATE:825)
```

- CSCdv63980

The VPN Client cannot use backup servers during connection attempts if it is configured to use IPSec over TCP for NAT Transparency (TunnelingMode=1).

- CSCdv75911

If the VPN Client is configured to use IPSec over TCP for NAT Transparency, (Tunneling Mode=1), you cannot establish a connection using PPP or Ethernet if you use a large certificate (such as one created by a Microsoft CA).

- CSCdv76902

If a session is already active when the Cisco Integrated Client firewall is enabled (either on the VPN Client or by policy pushed down from the Concentrator (CPP), that session is permitted to continue sending outbound packets, as long as they are not blocked by an outbound rule.

However, if the first packet sent after the firewall is enabled is inbound, the firewall does not allow the packet.

- CSCdv77711

On a Windows 95 PC the following error may occur during a connection:

CVPND caused an invalid page fault in module <unknown> at 0000:0400225b

If this message appears, reboot the computer. The VPN Client then connects to the Concentrator with no problem.

- CSCdv81538

If BlackICE Defender version 2.9 is on Windows XP and the VPN Client is reinstalled, the computer may display a blue screen (failure) upon reboot.

- CSCdv86123

If you are using the enroll command for certificates and you enter information in all fields, you might get a segmentation fault.

- CSCdx31313

The following error may occur on a Windows 95 PC when connected to the Concentrator:

CVPND caused an invalid page fault in module <unknown> at 0000:100022e5.

Registers:

EAX=00000102 CS=0137 EIP=100022e5 EFLGS=00010206

EBX=00000001 SS=013F ESP=011ED258 EBP=011EFF94

ECX=CB6F9ACC DS=013F ESI=00000000 FS=2757

EDX=CB6F9ACC ES=013F EDI=100022B6 GS=0000

Bytes at CS:EIP

- CSCdx39302

The Microsoft error messages that appear when you attempt to install the VPN Client using the Windows Installer do not indicate that Windows 95, Windows 98, Windows Me, and Windows NT (SP3) are not supported for Release 3.6 of the VPN 3000 Series Concentrator.

These errors occur on PCs that do *not* have the Microsoft Windows Installer installed (Windows 95, Windows 98 and Windows NT (SP3)) or that have an older version of MSI installed (Windows Me). Once the errors occur and you click OK, no other messages are displayed and the installation is aborted.

This is a Microsoft issue. The messages are as follows:

- On Windows 95 and Windows 98, when you attempt to run `vpnclient_en.exe` you see the following message:

“Cannot find the file MSIEXEC (or one of its components). Make sure the path and filename are correct and that all the required libraries are available.”

- On Windows NT SP3, when you attempt to run `vpnclient_en.exe` you see the following message:

“Cannot find the file `instmsiw.exe` (or one of its components). Make sure the path and filename are correct and that all the required libraries are available.”

followed by:

“Cannot find the file MSIEXEC (or one of its components). Make sure the path and filename are correct and that all the required libraries are available.”

- On Windows Me, when you attempt to run `vpnclient_en.exe` you see:

“This installation package cannot be installed by the Windows Installer service. You must install a Windows service pack that contains the newer version of the installer service”

- CSCdx50376

The following error message occurs if the MSI installation is canceled after DNE is installed but before the installation has completed:

“Error in Custom Action. The library CSGina.dll is invalid or could not be found.”

When this message appears, click OK; the rollback continues with no further errors.

- CSCdx58271

After installing the VPN Client using the MSI installer, rebooting, then launching the installer again, a box appears offering to Repair or Remove. If Repair is selected, the installer attempts to reinstall the Client. During the “Repair”, the following message box appears:

Deterministic Network Enhancer

Add plug-in failed

Click the OK button and another message appears:

Error 1722. There is a problem with this Windows Installer Package...

Click the OK button and the installer rolls back without another message.

NetworkICE and DNE are researching this issue.

- CSCdx60297

Using Auto-initiate to connect the client before logging into a domain on Windows 95 may result in no VPN Client tray icon appearing (yellow padlock). The client is connected and can be launched from the start menu to view status or disconnect

- CSCdx66747

If the VPN Client is uninstalled, the Computer must be rebooted before attempting to reinstall the Client. If the Computer is not rebooted between uninstalling and reinstalling the Client, the Client will not be able to connect to the Concentrator.

If this situation occurs, uninstall the Client, reboot the PC, then reinstall the Client and reboot after the reinstall.

- CSCdx83871

Using a LAN-to-LAN configuration with Digital Certificates, sending entire chain does not work. If set to send Ident only, it works fine.

- CSCdx86987

When using the VPN Client Certificate Manager to perform an SCEP enrollment to a CA that was previously enrolled to, the CA's URL appears incomplete as "http:/".

- CSCdx87075

The 3.6 VPN Client cannot connect with digital certificates if it is sending the certificate chain.

Workaround

Disable "Send CA certificate chain" on the client and manually install the certificates needed on the Concentrator to validate the client's ID certificate.

To disable Send CA certificate chain on the client, do the following:

Step 1 Click Options->Properties

Step 2 Change to the Authentication Tab and uncheck the option near the bottom of the dialog.

- CSCdx89079

If ZoneAlarm version 2.6.362 is installed on the PC the following Blue Screen might occur:

Stop: 0000001e (80000003, 80452e64, 00000000, 00000000)

kmode_exception_not_handled

***Address 80452e64 base at 80400000, datestamp 384d9b17 -- ntoskrnl.exe

- CSCdx89903

The VPN Client (using the Windows Installer - MSI) requires that Windows NT 4.0 users *must* use Service Pack 6 (SP6). The message that appears when installing on NT 4.0 SP3 - SP5 does *not* say that SP6 is required.

- CSCdx89962

Problems have occurred on some Windows NT systems when using AES encryption. The PC may blue screen after sending data using AES. The problem is under investigation.

Workaround:

Add the following line into the vpnclient.ini file in the [Main] section and restart the computer:

ExcludeAESProps=1

The vpnclient.ini file is in the following directory:

c:\Program Files\Cisco Systems\Vpn Client

This line keeps the VPN Client from sending any AES proposals to the Secure Gateway that keep AES from being negotiated. Keep in mind that the Secure Gateway must be configured for a different encryption protocol.

- CSCdx92053

The Windows Installer (MSI) version of the v3.6 VPN Client install does not register IPSECDIALER.EXE in the following registry key as previous versions of the VPN Client did:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\ipsecdialer.exe

This occurs *only* when using the Windows Installer (MSI). The InstallShield version does not exhibit this problem.

- CSCdy08772

The VPN Client is adding bogus information into the Backup Server list when the VPN 3000 Concentrator sends a list of backup servers and is configured to use the list. If you look in the .PCF file after a connection, you will see something similar to this:

BackupServer=200.70.50.199,200.70.50.200,200.70.50.250,Version,3.6.int_76,built,by,yurname,on,Jul,02,2002,19:00:2400.compp

Documentation Updates

The following VPN Client documentation has been updated for Release 3.6. These documents contain information for all platforms on which the VPN Client runs:

- *VPN Client Administrator Guide, Release 3.6*
- *VPN Client User Guide for Windows, Release 3.6*

The most recent information specifically for the VPN Client for Linux, Solaris, and Mac OS X is in the following document, which was not updated for Release 3.6:

- *Cisco VPN Client User Guide for Linux, Solaris, and Mac OS X*

Related Documentation

- *VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 3.6*
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Management, Release 3.6*
- *VPN 3000 Series Concentrator Getting Started, Release 3.6*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

Copyright and Trademark Information

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.